usecure

7 SIGNS YOU'RE BEING PHISHED!

Some common warning signs of a potential phishing email.

The email is poorly written

Although scammers can accidentally fall short in the grammar department, these 'mistakes' aren't always unintentional. Errors can be purposefully included in order to limit interaction with only the more 'observant'.

It contains unsolicited attachments

Typically, authentic institutions don't randomly send emails with attachments, especially when there is no previous relationship involved. If in doubt, contact the legitimate company by searching for their website.

It requests sensitive information

Emails that ask you to send sensitive info, such as banking details, tax scores or login credentials, are seriously phishy. You should search online and contact the organisation directly - not the sender.

There's urgency involved

Some scammers try to inflict urgency in their emails - often with threats of account expiration, fines or even prize giveaways - to encourage us to make rash decisions without proper thought.

It sounds to good to be true

Scammers often include 'limited' and 'unmissable' prize giveaways in their phishing emails in an attempt to blur our safety glasses. How does the old adage go? "If it sounds to good to be true...".

It doesn't address you by name

Many phishing scams are sent in their masses, with none (or limited) personalisation involved.

The email address looks altered

Scammers can make their email address look legitimate by including the company name within the structure of their email (e.g john@paypal123.com). Hover over links to make sure they don't look altered.